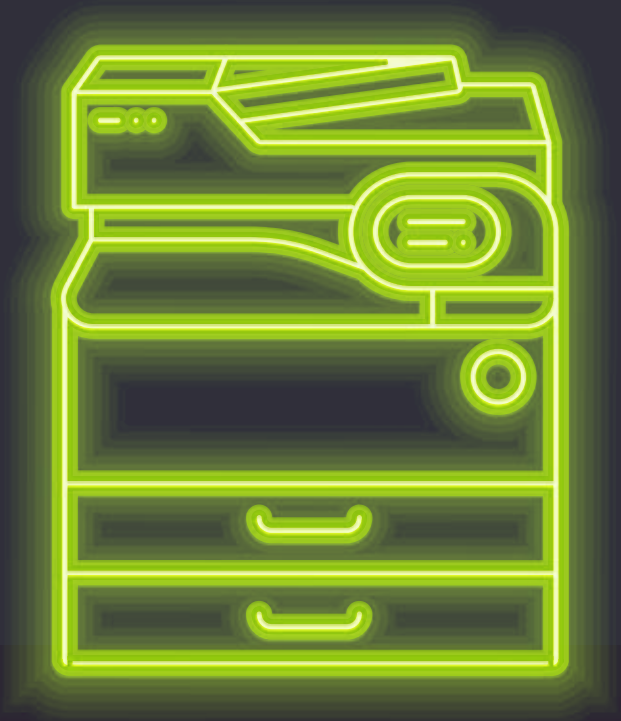
Druckersicherheit: Das neue IT-Problemfeld

Studie zeigt, dass Sicherheitsgefahren durch den „einfachen Drucker“ nach wie vor ignoriert werden



dtb office solutions seit 1996

Inhaltsverzeichnis

Einführung

Während die Bedrohungen für die IT-Sicherheit zunehmen, fallen die Sicherheitsvorkehrungen für die Hardware oft zurück. Vermutlich wird das nirgendwo so deutlich wie bei Druckern. Obwohl IT-Fachleuten die zunehmende Gefahr bewusst ist, die durch ungeschützte Drucker im Netzwerk entsteht, bleiben Drucker ein sicherheitstechnischer blinder Fleck und sind in den meisten Fällen zu wenig geschützt.

„Schwachstellen zeigen sich in allen möglichen Geräten innerhalb eines Netzwerks, sogar beim einfachen Netzwerkdrucker“, erklärt der Geschäftsführer für Drucksysteme bei HP South Pacific, Ben Vivoda. **„Der Drucker ist ein typischer Fall für Geräte, die übersehen werden und dadurch exponiert sind. Unternehmen können es sich nicht länger erlauben, die Drucker in ihrer Gesamtstrategie für Cybersicherheit zu übersehen.“**[1]

Tatsächlich sind Drucker laut einer aktuellen Studie von Spiceworks zunehmend Ursache für zahlreiche Bedrohungen der Sicherheit. Im Vergleich zu 2016 liegt die Wahrscheinlichkeit, dass Drucker die Ursache für externe Bedrohungen oder Angriffe sind, 68 % höher. Bei internen Bedrohungen oder Angriffen ist die Wahrscheinlichkeit sogar um 118 % gestiegen.

Und doch sind sich nur 30 % der IT-Profis bewusst, dass Drucker ein Sicherheitsrisiko darstellen. Dieser Anteil hat sich seit 2016 zwar ungefähr verdoppelt, ist aber immer noch zu niedrig und spiegelt eine gefährliche Wirklichkeit wider. Viele IT-Profis haben offensichtlich immer noch veraltete Ansichten zur Druckersicherheit. Vielleicht weil sie denken, dass Drucker innerhalb eines Netzwerks geschützt sind.

Selbst für IT-Profis, denen das Risiko bewusst ist, hat die Sicherheit der zahllosen Endnutzergeräte höchste Priorität, sodass Drucker außen vor bleiben und Netzwerke verwundbar werden.[2] Obwohl es verständlich ist, dass die Druckersicherheit in der Vergangenheit verglichen mit anderen Endpunkten eine untergeordnete Rolle spielte, müssen IT-Abteilungen unbedingt anfangen, das Risiko ungeschützter Drucker für die IT-Infrastruktur und die Risikobeherrschung im Unternehmen anzugehen.

Die Risiken des Geschäfts

Sind Drucker wirklich ein Problem? Kurz gesagt: Ja. In einer Zeit, in der stündlich neue Sicherheitsbedrohungen auftauchen, ist der Drucker ein leichtes Ziel. „Moderne Drucker sind im Grunde fortschrittliche, spezialisierte Netzwerk-Hosts, die die gleiche Aufmerksamkeit in puncto Sicherheit verdienen, wie herkömmliche Computer“, führt Kevin Pickhardt in Entrepreneur aus.[2] „Bürodrucker sind nicht nur potenzielle Quellen für Datenverlust und Vertraulichkeitsprobleme, sondern auch Angriffsvektoren, die Hacker ausnutzen können.“ Nur ein Beispiel: Letztes Jahr nutzte ein Hacker ein automatisiertes Script, um Zugriff auf 150.000 öffentlich zugängliche Drucker einschließlich zahlreicher Belegdrucker zu erlangen und ihnen fehlerhafte Druckaufträge zu erteilen.[3]

Branchenkenner sind derselben Meinung. Laut IDC verfügen die meisten Drucker über „umfassenden Zugriff auf das interne Netzwerk. **Ein Angreifer, der einen Drucker kapert, kann sich ungehinderten Zugriff auf das Netzwerk, Anwendungen und sensible Daten eines Unternehmens verschaffen.“**[4]

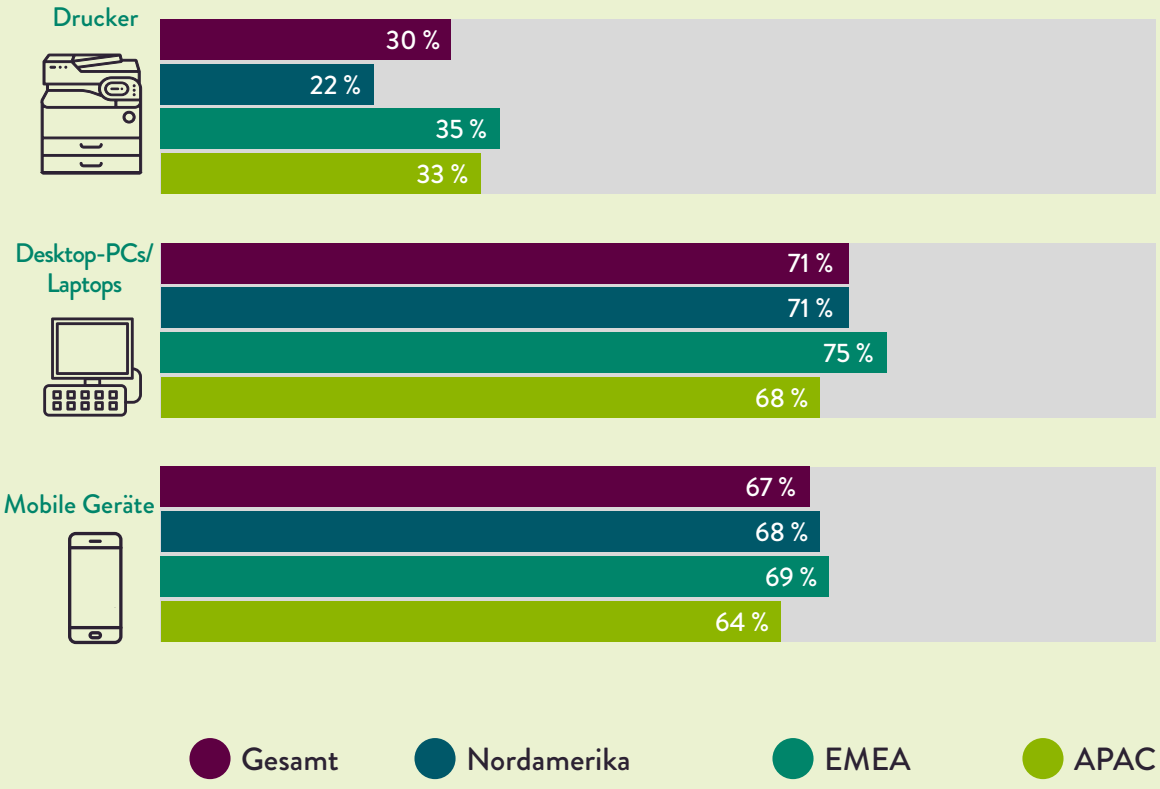
Woran erkenne ich einen Netzwerkdrucker, der nicht ausreichend geschützt ist? Er ist nicht abgesichert und dadurch weit offen für zahllose Netzwerkprotokolle. Er erfordert keine Zugriffskontrolle (selbst das Anlegen eines Admin-Passworts wird oft übersehen). Er ermöglicht das Drucken sensibler Dokumente ohne Authentifizierung, sodass die Dokumente den ganzen Tag für jedermann zugänglich im Ausgabefach liegen bleiben können. Er versendet unverschlüsselte Daten im Netzwerk. Seine Firmware ist veraltet oder wird nicht auf Sicherheitsbedrohungen überwacht.

All diese Sicherheitsmängel haben Folgen. Gartner sagt voraus, dass bis 2020 mehr als die Hälfte aller Projekte zum Internet der Dinge (IoT) sensible Informationen dadurch preisgeben, dass die Sicherheitsfunktionen der Hardware nicht genutzt werden. Heute sind es weniger als 5 %.[4]

Fehlendes Problembewusstsein

Trotz dieser Forschungsergebnisse tun sich IT-Profis nach wie vor schwer, die Risiken zu erkennen, die Drucker darstellen. In Nordamerika sehen nicht einmal ein Viertel aller IT-Profis (22 %) Drucker als Sicherheitsrisiko. In Europa, im Mittleren Osten und Afrika (EMEA) ist diese Zahl mit gut einem Drittel (35 %) nur unwesentlich höher.

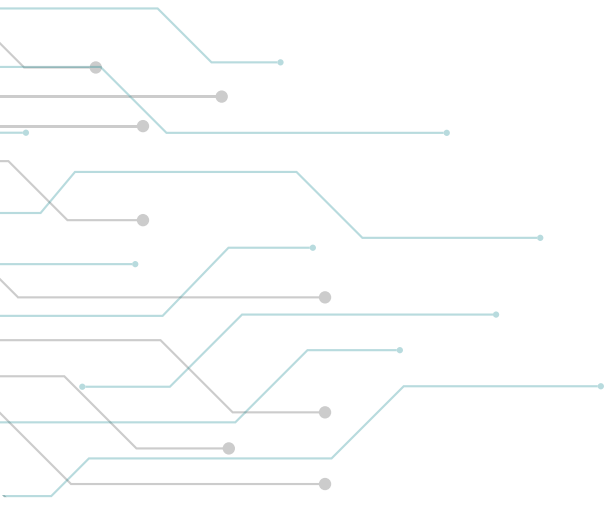
Als Sicherheitsrisiko erkannt



Im Gegensatz dazu, erkennen 71 % der IT-Profis das Risiko durch Desktop-PCs und Laptops und 67 % durch Mobilgeräte.

Die Forschungen von Spiceworks decken zudem auf, dass die IT-Profis, die vorbeugende Maßnahmen ergriffen haben, keinen zusammenhängenden Ansatz wählten. Das ist angesichts der vielen unterschiedlichen Sicherheitsanforderungen auch kein Wunder. Eine einfache Lösung reicht nicht. Zum Beispiel ist es lediglich mit einer Firewall noch nicht getan. Wie bei allen Netzwerkgeräten muss die Druckersicherheit von vielen Seiten aus angegangen werden. Und wie bei jeder Sicherheitsstrategie sind die effektivsten Lösungen integriert, automatisiert und einfach zu bedienen und zu verwalten.

Noch komplizierter wird die Sache dadurch, dass jeder Druckerhersteller seine eigene Software und sein eigenes Betriebssystem nutzt. Viele IT-Profis besitzen wahrscheinlich nicht genügend Know-how, um die Druckersoftware so zu konfigurieren, dass die Sicherheitsrichtlinien erfüllt werden.



Gängige Praxis

IT-Profis verfolgen verschiedene Ansätze in Richtung Druckersicherheit, was zu einem heillosen Durcheinander aus Sicherheitsverfahren und -funktionen auf Basis von Tools führt, die ihnen zur Verfügung stehen und die sie verstehen. Im Großen und Ganzen lassen sich die Ansätze für die Druckersicherheit aber in sechs Kategorien einordnen.

Anteil der Teilnehmer, die zurzeit folgende Sicherheitspraktiken für Drucker anwenden

42 % Dokumentensicherheit

31 % Gerätesicherheit

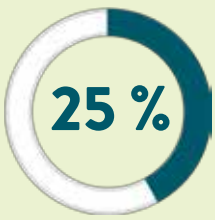
40 % Netzwerksicherheit

30 % Sicherheitsüberwachung

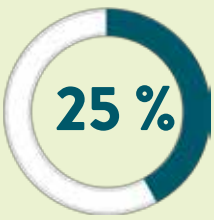
39 % Zugriffssteuerung

28 % Datenschutz

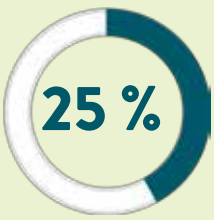
Die Studie hat gezeigt, dass IT-Profis verschiedene grundlegende Sicherheitsschritte in diesen Kategorien einleiten, allerdings zu einem sehr geringen Anteil.



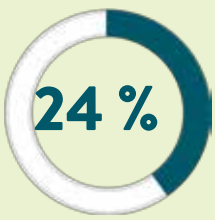
Schließen ungenutzter offener Ports



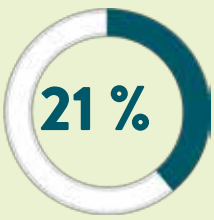
Aktivieren der Funktion „gesendet von“



Sichere Druckerreparaturen



Einführung von geschütztem Drucken („Pull-Printing“)

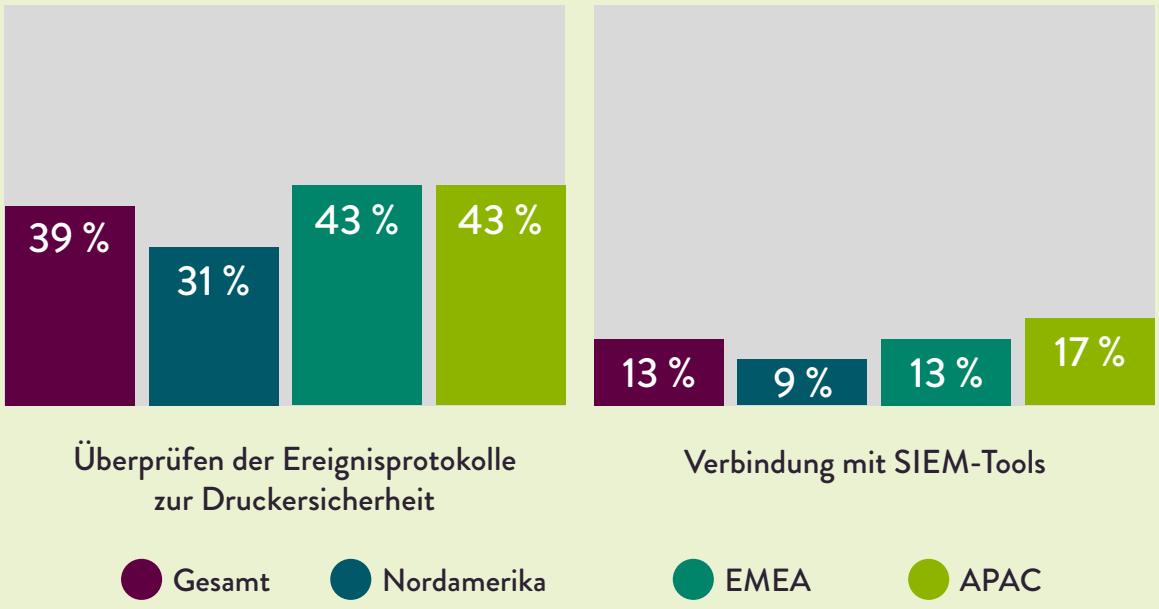


Routinemäßiges Löschen der Druckerfestplatte

Noch geringer ist die Zahl der IT-Profis, die Druckaufträge regelmäßig verfallen lassen oder löschen, einen Admin-Zugang für Änderungen an der Konfiguration anlegen oder die Zertifikatsverwaltung automatisieren.

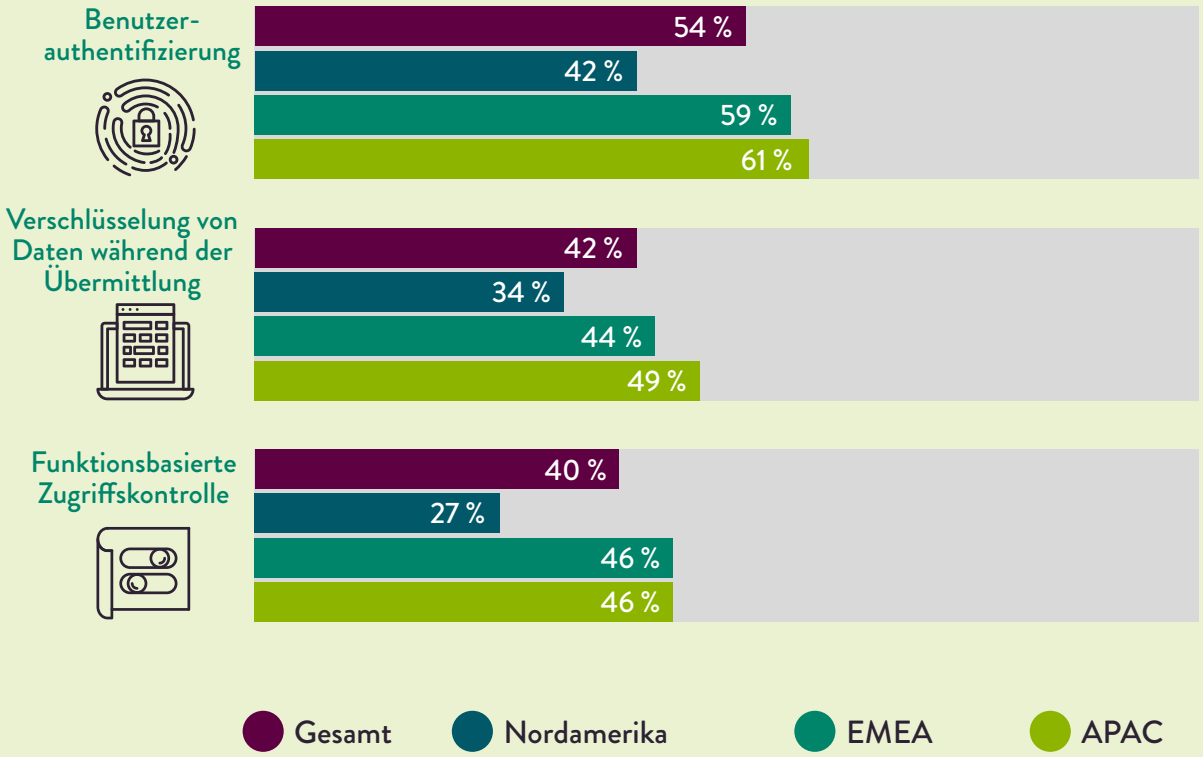
IT-Profis führen inzwischen häufiger Überwachungen der Druckersicherheit durch, aber der Anteil von 39 % der IT-Profis, die angeben, die Druckerprotokolle routinemäßig zu prüfen, ist immer noch gering. In Nordamerika sind es nur 31 %. In Bezug auf die Verbindung von Druckern mit SIEM-Tools, geben nur 13 % an, dies vorgenommen zu haben. Dadurch, dass Druckerprotokolle nicht überwacht und Drucker nicht in SIEM-Tools integriert werden, tappen IT-Profis im Dunkeln und übersehen Cyberkriminalität, die unbewachte Infrastruktur als Versteck in einem Netzwerk nutzt, um Daten herauszufiltern.

Druckerüberwachung



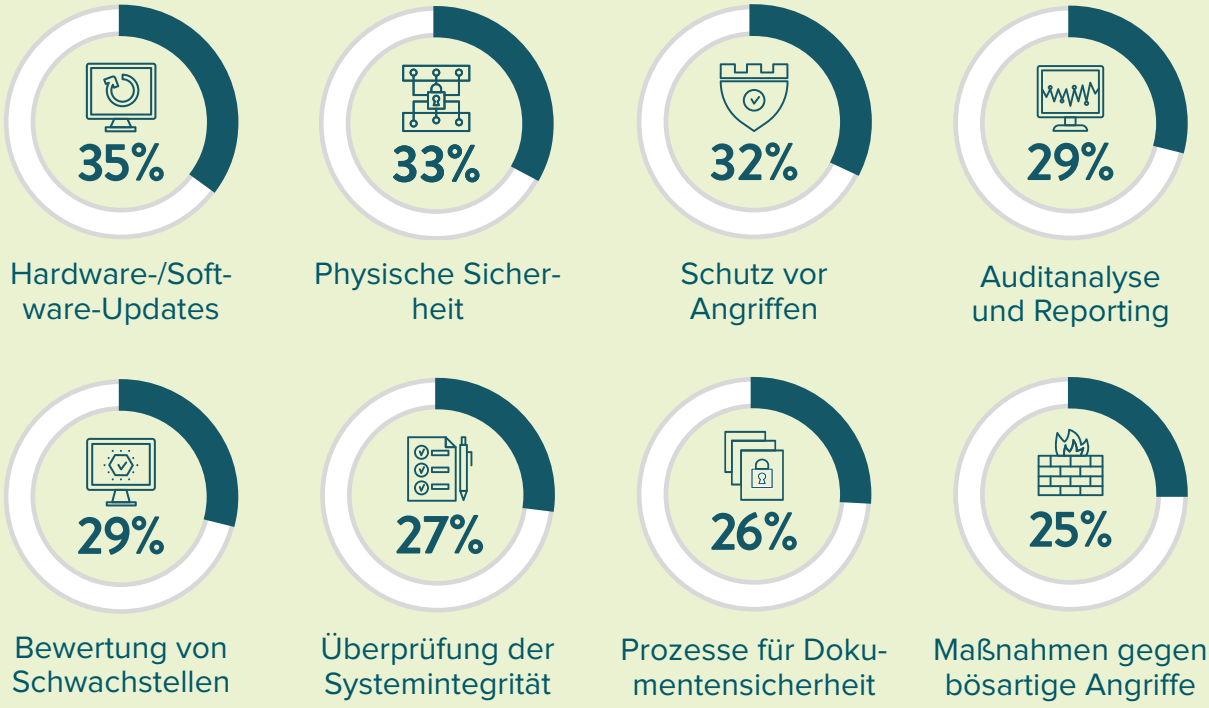
Die Studie hat weitere Unterschiede zwischen den Regionen bei der Druckersicherheit aufgedeckt – und wieder liegt Nordamerika hinten. Dies gilt besonders für Zugriffskontrollen und die Verschlüsselung. IT-Profis in APAC verschlüsseln mit deutlich höherer Wahrscheinlichkeit ihre Daten bei der Übertragung als in Nordamerika, sie verlangen häufiger eine Authentifizierung auf Geräteebene und vergeben Zugriffsrechte auf Grundlage der Funktion der Nutzers.

Praktiken zur Druckersicherheit eingerichtet



Zu guter Letzt setzen IT-Profis für die Einhaltung von Datenschutzbestimmungen wiederum auf verschiedene Ansätze, wenn z. B. einige Druckerkontrollen in die Gesamtstrategie zur IT-Compliance eingebunden werden. Die Spiceworks Studie fragte IT-Profis, welche Compliance-Kontrollen sie auf Basis von „CIS Controls V7“ des Center for Internet Security umgesetzt haben.[5]

Compliance-Kontrollen eingerichtet



Die Daten zeigen, dass IT-Profis oft die grundlegendsten Vorsichtsmaßnahmen für Drucker übersehen, z. B. die Aktualisierung der Firmware. Nur ein Drittel erklärt, diese Aufgabe im Rahmen der Compliance-Routine auszuführen. Branchenstudien zeigen dieselben Ergebnisse. Laut IDC wird die Firmware bei Druckern häufig nicht aktualisiert, weil die Unternehmen das Risiko sehr oft unterschätzen.[4] Hinzu kommt, dass ihnen häufig die Zeit fehlt, um die neue Firmware für sämtliche Drucker im Bestand zu prüfen, zu testen und abzunehmen.

Auf dem Weg zu umfassender Druckersicherheit

Von den 84 % der IT-Profis, in deren Unternehmen eine Sicherheitsrichtlinie festgelegt ist, geben nur 64 % an, dass die Druckaufgaben in dieser Richtlinie aufgeführt sind. In Nordamerika sind es nur 52 %. Dies ist einer der Gründe, warum es so wichtig ist, integrierte und automatisierte Kontrollen zur Druckersicherheit zu ermitteln und tatsächlich umzusetzen. Drucker mit eingebauten Sicherheitsfunktionen minimieren zwar Ihr Risiko, maximieren aber gleichzeitig Ihre IT-Ausgaben.

Die IDC-Analysten haben auch diese Aussage ermittelt: „Drucker sind deutlich schwieriger zu sichern, nachdem sie ausgeliefert wurden, was nochmal die Bedeutung bei der Auswahl der Drucker hervorhebt, die bereits über umfangreiche und moderne Sicherheitsfunktionen verfügen.“[4] Gartner führt aus: „Um die entstehende Marktdynamik für Drucker zu nutzen, müssen die technologie-strategischen Planer ein umfassendes Portfolio an Sicherheitslösungen für Drucker bauen und hierfür Lösungsreihen einsetzen, die die gängige Praxis in der Sicherheitsbranche übertreffen. Diese Lösungen müssen in das Gesamtsystem für Sicherheitslösungen integriert werden.“[6]

Anbieter von Druckermanagementdiensten weiten ihren Service aus, um IT-Abteilungen zu unterstützen, die personell nicht so breit aufgestellt sind, dass sie Druckersicherheit bewältigen können. Wir zitieren nochmal IDC: „Auf dem Markt ist eine breite Palette von Services für den Schutz auf Geräte- und Datenebene erhältlich, die sich häufig in bestehende Systeme für das Management von Dokumenten und Unternehmensinhalten (Enterprise Content Management, ECM) integrieren lassen, um den Schutz zu erweitern und die Governance sowie die Einhaltung gesetzlicher Bestimmungen zu erleichtern.“[7]

Zum Glück für IT-Profis bieten die modernen Drucker von heute dutzende integrierte Sicherheitsfunktionen für das Drucksicherheitsportfolio: Erkennung von Bedrohungen, Schutzmaßnahmen, Benachrichtigungen und eigenständige Fehlerbehebung – all das macht es so einfach wie nie, die Schwachstelle in Ihrem Netzwerk sicher zu machen, nämlich den einfachen Drucker.

Es ist an der Zeit, Ihren Druck-Workflow sicher zu machen

Weitere Informationen

Über die Studie

HP beauftragte Spiceworks mit der Durchführung der Studie im Mai 2018. Sie zielt auf Entscheidungsträger im IT-Bereich, einschließlich IT-Bereichsleiter, IT-Manager und andere IT-Mitarbeiter um zu ermitteln, welche Sicherheitspraktiken zurzeit genutzt werden und welche Risikobereiche bestehen. Die Studienergebnisse spiegeln die Antworten von ca. 500 Teilnehmern in Nordamerika, EMEA und APAC wider, die in Unternehmen mit mehr als 250 MitarbeiterInnen beschäftigt sind.

Quellen

1 McLean, Asha, „Unsecured printers a security weak point for many organisations: HP“ ZDNet, 18. April 2017. https://www.zdnet.com/article/unsecured-printers-a-security-weak-point-for-many-organisations-hp/

2 Pickhardt, Kevin, „Why Your Innocent Office Printer May Be a Target For Hackers“ Entrepreneur, 31. Januar 2018. https://www.entrepreneur.com/article/308273

3 Peyser, Eve, „Hacker Claims He Hacked 150,000 Printers to ‘Raise Awareness’ About Hacking“ Gizmodo, 6. Februar 2017. https://gizmodo.com/hacker-claims-he-hacked-150-000-printers-to-raise-aware-1792067012

4 Brown, Duncan, et al., „IDC Government Procurement Device Security Index 2018“ IDCMai 2018.

5 „CIS Controls“ Center for Internet Security, März 2018. https://www.cisecurity.org/controls/

6 Von Manowski, Kristin Merry und Deborah Kish, „Market Insight: IoT Security Gaps Highlight Emerging Print Market Opportunities“ Gartner, 31. Oktober 2017 https://www.gartner.com/doc/reprints?id=1-4OCKFKG&ct=180110&st=sb

7 Palmer, Robert und Allison Correia, „IDC MarketScape: „Worldwide Security Solutions and Services Hardcopy 2017 Vendor Assessment“* IDC, 2017.